REMARKS

This Reply is responsive to the Office Action[1] having a mailing date of May 4, 2006. Claims 1-6 and 8-22 were presented for examination in this second Request for Continued Examination and were rejected. Claims 1, 5, 9, 13, 14 and 22 are independent claims and are amended. No new matter is added as explained below. No claims are canceled or added. Thus, claims 1-6 and 8-22 are pending.

Claims 1-6 and 8-22 are now rejected under 35 U.S.C. § 103(a) as being un-patentable over Sudia et al. (U.S. Patent No. 5,825,880; hereinafter "Sudia") and further in view of Veil et al. (U.S. Patent No. 6,092,202, hereinafter "Veil"). The rejection is respectfully traversed for at least[2] the following reasons.

Consider previously presented claim 1:

> In a node operative within a network of a plurality of nodes, a method for performing cryptographic-related functions, comprising: executing an application program at the node which is *not physically secured*; receiving an input requiring cryptographic-related processing; generating a message via the application program based on the input, the message representing one of a predefined set of messages for processing by a cryptographic processing component located within the node; transmitting the message to the cryptographic processing component; and performing the cryptographic-related processing by the cryptographic processing component. (Emphasis added.)

Claim 1 calls for, interalia, executing an application program at a node that *is not physically secured*. Sudia taken alone or in combination with Veil does not disclose or

[1] The Office Action may contain a number of statements characterizing the cited references and/or the claims which Applicants may not expressly identify herein. Regardless of whether or not any such statement is identified herein, Applicants do not automatically subscribe to, or acquiesce in, any such statement.

[2] Other arguments previously presented in this prosecution are still viable, even if not re-asserted herein; for example, arguments presented with respect to Sudia's not completely performing its security function within a network node as compared with Applicants' complete performance of its security function within a network node is a position which Applicants continue to maintain, despite its absence from the instant remarks; Applicants reserve their rights to make further arguments therefor if Applicants choose to do so.

suggest executing an application program at a node which is not physically secured, as explained below.

To begin with, Applicants had previously amended claim 1 by changing "executing an application program at the node which need not be highly secured" to "executing an application program at the node which is not highly secured" to "executing an application program at the node which is not secured." That has now been changed in the current amendment to "executing an application program at the node which is not physically secured." To be clear, claim 1 presently recites methodology operating in a **physically unsecured** node.

In response to the last amendment, the Examiner admits in the Office Action that "Sudia further teaches executing an application program at the node which is not highly secured"(Office Action, page 4) and further admits "However, [Sudia] did not go into details the node is not secured." (Office Action, page 4) In other words, the Examiner further admits that Sudia does not teach that its node is not secured, and Applicants agree. Based on this admission, the Examiner found it necessary to change the grounds of rejection from 35 U.S.C. §102(b) to 35 U.S.C. §103(a) in the Office Action, citing Veil.

But, Veil also teaches secure transactions in a computer system. (Title and Abstract) Per the Office Action, "Veil teaches an invention for providing secure transaction in a computer system and environments within these transactions (col. 3, line 66 - col. 4, line 3)." (Office Action, page 4, Emphasis added.). Therefore, even the Office Action admits that Veil teaches secure transactions. Nevertheless, despite the teachings of secure transactions in Veil, the Examiner relies on the following section of Veil to support the new grounds of rejection:

> A majority of the application programs for conducting electronic transactions (electronic transactions applications) are executable on one of the conventional operating system platforms such as OS/2.RTM., Windows.RTM., UNIX.RTM. etc. It is generally known that conventional operating system platforms provide a non-secure computing environment for executing the electronic transactions applications. In the non-secure computing environment, confidential information related to the electronic transactions (sensitive data) can be easily compromised. (Veil, column 4, lines 27-36, Emphasis added.)

This section of Veil merely discusses the problem which is allegedly solved by Veil. In other words, the disclosure of Veil overwhelmingly has to do with secure transactions and the provision of a security co-processor to overcome the security deficiency alluded to in the above-quoted section. The above section merely describes the problem that Veil is addressing.

Moreover, this section in Veil discusses no more than conventional operating systems (computer software) which may result in an insecure software environment and therefore carries no weight in countering the *physical* security teachings of Sudia. Indeed, Sudia teaches operational security based on "vaults" and on tamper-proof "smartcards" etc. For example, a principal teaching of Sudia is that the authorizing agent and the signing device are required to be physically separated for security purposes, and are separated even to the extent that the signing device of, e.g., Fig. 1, is located in a physically secure location such as a *vault* (Sudia. Col. 7, lines 24-25). Security-shortcomings of conventional operating system performance do not counter this physical security notion.

This physical-separation aspect of security is reinforced throughout Sudia. Consider, for example, "no private signature key exists at a single location where it may

be subject to compromise or catastrophe. Multiple sites must fail or be compromised before interrupting signing services or before an adversary acquires sufficient information to forge signatures." (Sudia, Col. 3, lines 22-27, Emphasis added.) Security-shortcomings of conventional operating system performance do not counter this physical security notion.

Furthermore, Sudia's smart card is touted as being secure: "Each such computer or terminal will have a card reader 53, and each operator will have a *secure* 'smart card' 55. Each smart card 55 *securely* contains a private decryption key and a private signature key which are unique to that smart card." (Sudia, Col. 8, lines 23-27, Emphasis added.) The smart cards are said to be "tamper-resistant." *See*, for example, Sudia, column 3, line 30, or column 9, lines 41-49. Security-shortcomings of conventional operating system performance do not counter any physical security notion associated with tamper resistance.

Accordingly, this brief reference in Veil to limitations of conventional operating system platforms allowing a non-secure computing environment does nothing to counter the teachings in Sudia of physically secure or physically highly secure environments. Conventional operating system performance (computer software operation) has no direct relationship to physical security such as, e.g., that based on separate physical locations. Thus, even if these references were combinable, and Applicants do not concede that these references are properly combinable in the first place, their combined teachings would not disclose or suggest the subject matter in Applicants' currently amended claim 1.

To the contrary, if a combination of the two references were attempted, the secure transaction processing being performed in the security co-processor in Veil, and any

other security discussion in Veil, would actually ADD to the security picture in Sudia. After all, Sudia teaches security and Veil teaches security. In such a case, an augmented security environment resulting from that combination would actually teach away from the "node which is not physically secured" language recited in Applicants' claim 1. Indeed, the references, taken alone or in combination, do not disclose or suggest: "executing an application program at the node which is not physically secured" as recited in claim 1. Therefore, the 35 U.S.C. §103(a) rejection of claim 1 should be withdrawn and the claim allowed.

Applicants' claim amendment language, "...the node is not physically secured" is supported by the application as originally filed. For example, in Applicants' specification, page 6, lines 1-3, it discusses the nodes 110, 120, and 130 of Fig. 1, such nodes along with server 140 and network 150 comprising Applicants' system. As stated therein, those nodes can be any type of computer device. For example, as disclosed therein, those nodes can be "a personal computer, a laptop, a personal digital assistant (PDA) or a similar device with a connection to network 150." Clearly, these examples of nodes from which Applicants' claimed subject matter can be implemented are not used in a physically secure environment - e.g., people using a laptop or a PDA do not first find their way to a "vault" and then place themselves with their laptop or PDA inside the vault for physical security purposes before operating their laptop or PDA. Far to the contrary, laptops and PDA's are used in virtually all public spaces such as, for example, airports, airplanes, trains and train stations, buses and bus depots, taxis, hotels lobbies, corporate business environments, etc. Therefore, Applicants' specification as originally filed

clearly supports the notion that the "nodes" of its system are used without their being physically secured, as recited in amended claim 1.

The other independent claims, claims 5, 9, 13, 14 and 22 each contain a recitation that is the same as, or similar to, the "node which is not physically secured" language of claim 1. Therefore, these other independent claims, rejected as being un-patentable over the same two references, are allowable for the same, or similar, reasons as those given above with respect to claim 1.

Therefore, claims 2-4 dependent from claim 1, claims 6 and 8 dependent from claim 5, claims 10-12 dependent from claim 9, and claims 15-21 dependent from claim 14 are also allowable, at least for reasons based on their dependencies from allowable base claims.

CONCLUSION

In view of the foregoing remarks, reconsideration and allowance are respectfully requested. Applicants respectfully request withdrawal of the outstanding rejections and the timely allowance of this application.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 07-2347 and please credit any excess fees to such deposit account.

Respectfully submitted,

By: /Eden U.I. Stright/, Reg. No. 51,205 for
Joel Wall
Reg. No. 25,648

Date: August 1, 2006
Verizon
Patent Management Group
1515 Courthouse Road, Suite 500
Arlington, VA 22201-2909
Tel: 703.351.3586
CUSTOMER NO. 32127